

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

**CHAMBERS OF
MADELINE COX ARLEO
UNITED STATES DISTRICT JUDGE**

**MARTIN LUTHER KING COURTHOUSE
50 WALNUT ST. ROOM 4066
NEWARK, NJ 07101
973-297-4903**

September 21, 2023

VIA ECF

LETTER ORDER

**Re: IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC.
CUSTOMER DATA SECURITY BREACH LITIGATION
Civil Action No. 19-md-2904**

Dear Litigants:

Before the Court are Motions to Dismiss an Amended Consolidated Class Action Complaint (the “FAC”), ECF No. 317, filed in connection with the instant multidistrict litigation (“MDL”) by: (1) OPTUM360, LLC (“Optum”), ECF No. 349; and (2) Quest Diagnostic Incorporated (“Quest”), ECF No. 350 (the “Motions”).¹ For the reasons set forth below, the Motions are **GRANTED IN PART** and **DENIED IN PART**.

I. BACKGROUND²

This MDL arises from a data breach suffered by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency (“AMCA”). See generally FAC. Defendants are primarily healthcare providers who hired AMCA as a collections vendor and provided AMCA with sensitive patient information to facilitate collections. Between late 2018 and March 2019, an unauthorized user or users gained access to an AMCA computer system containing the private information of millions of patients (the “Data Breach”). Plaintiffs are among those patients whose Personal Information was impacted by the Data Breach. Each FAC alleges claims against a different Defendant or group of Defendants.

On December 16, 2021, the Court granted in part and denied in part motions to dismiss the original consolidated class action complaints (“CCAC’s”). See generally, 2021 Opinion. The Court identified three groups of plaintiffs: (1) patients who had allegedly suffered economic injuries resulting from the misuse of their Personal Information (the “Group I Plaintiffs”); (2) patients who did not experience direct economic harm, but who alleged facts sufficient to infer that an unauthorized user obtained the patient’s Personal Information in the Data Breach (the

¹ The Court notes that it has also reviewed of the parties’ recent supplemental briefing.

² As the Court has addressed the facts of this case in detail in its December 16, 2021 Opinion, ECF. No. 283 (the “2021 Opinion”), and its May 5, 2023 Order, ECF No. 507 (the “2023 Order”), the Court summarizes only the facts necessary to address the present Motions.

Group II Plaintiffs"); and (3) patients who alleged that their Personal Information was stored in the compromised AMCA systems but do not allege any other facts to suggest that their information was actually accessed, downloaded, or misused by an unauthorized party (the "Group III Plaintiffs").³ The Court dismissed the claims of the Group III Plaintiffs for lack of standing because they did not allege an injury-in-fact. The Court held that the remaining Plaintiffs had sufficiently pled negligence, negligence *per se*,⁴ and certain state statutory violations,⁵ but did not sufficiently plead unjust enrichment and breach of implied contract.

On March 31, 2022, Plaintiffs filed an FAC against Quest and Optum asserting five common law claims: (1) negligence, (2) negligence *per se*, (3) breach of confidence, (4) invasion of privacy and (5) unjust enrichment. The FAC also asserts violations of state consumer laws.⁶ The instant Motions followed.

II. LEGAL STANDARD

1. Motion to Dismiss Under Rule 12(b)(1)

A motion to dismiss for lack of standing is properly brought pursuant to Rule 12(b)(1). See Bellentine v. United States, 486 F.3d 806, 810 (3d Cir. 2007). Under Rule 12(b)(1), a plaintiff bears the burden of persuading the Court that subject matter jurisdiction exists. See Kehr Packages, Inc. v. Fidelcor, Inc., 926 F.2d 1406, 1409 (3d Cir. 1991). In resolving a Rule 12(b)(1) motion, a court first determines whether to deem the motion a "facial" or "factual" attack. See Constitution Party of Pa. v. Aichele, 757 F.3d 347, 357 (3d Cir. 2014). A facial attack argues that

³ Group III includes 17 Quest Plaintiffs: (i) Ella Gulley, (ii) Moises Perez, (iii) William Infield, (iv) Annie Mae Smith, (v) Shannon Walden, (vi) Lucinda Dirks, (vii) Ashley Finch, (viii) Carolyn Green, (ix) Rose Marie Perry, (x) LaTease Rikard, (xi) Naomi Jaworowski, (xii) Cynthia Connor; (xiii) Karli Parker, (xiv) Deanna Taylor, (xv) William Lindsay, (xvi) Brittney Petitta, and (xvii) Jo Ann Buck.

⁴ Specifically, the Court found that the negligence and negligence *per se* claims of the following Plaintiffs against Quest and Optum could proceed: Julio Antonio Perez Vieyra, Elizabeth Hollway, Ria Jairam, Ann Davis, Noel Benadom, Nancy Infield, Michael Rutan, John Briley, Joyce Rosselli, and Darlane Saracina.

⁵ Specifically, the Court found that the consumer statutory claims of the following Plaintiffs against Quest could proceed: Elizabeth Hollway's Minnesota Consumer Fraud Act claim, and Julio Antonio Perez Vieyra's California Consumers Legal Remedies Act and the California Unfair Competition Law claims. The Court also found that Ria Jairam's claim against Optum360 under the New Jersey Customer Security Breach Disclosure Act could continue.

⁶ Plaintiffs claim violations of: (i) California's Confidentiality of Medical Information Act, Cal. Civ. Code §56, *et seq* ("CMIA"); (ii) California Unfair Competition Law, Cal. Bus. & Prof. Code §§17200, *et seq.* ("UCL"); (iii) California's Consumers Legal Remedies Act, Cal. Civ. Code §§1750, *et seq.* ("CLRA"); (iv) Indiana Unfair Trade Practices Act, Indiana Code § 24-5-0.5 ("INDPA"); (v) Iowa's Personal Information Security Breach Protection Law, Iowa Code § 715C.2 ("IPISBPL"); (vi) Iowa's Private right of Action for Consumer Frauds Act, Iowa Code § 714H ("IPRACF"); (vii) Kansas's Protection of Consumer Information, Kan. Stat. Ann. §§50-7a02(a), *et seq.* ("KPCI"); (viii) Kansas Consumer Protection Act, K.S.A. §§50-623, *et seq.* ("KSA"); (ix) Kentucky Computer Security Breach Notification Act, Ky. Rev. Stat. Ann. §§365.732, *et seq.* ("KCSBNA"); (x) Kentucky Consumer Protection Act, Ky. Rev. Stat. §§367.110, *et seq.* ("KCPA"); (xi) Michigan's Consumer Protection Act, Mich. Comp. Laws Ann. §§ 445.903, *et seq.* ("MICPA"); (xii) Minnesota's Consumer Fraud Act, Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.* ("MNCFCA"); (xiii) Missouri's Merchandising Practices Act, Mo. Rev. Stat. §§ 407.010, *et seq.* ("MOMPA"); (ixx) New Hampshire's Notice of Security Breach, N.H. Rev. Stat. Ann. §§ 359- C:20(I)(A), *et seq.* ("NHNSB"); (xx) New Hampshire's Consumer Protection Act, N.H.R.S.A. §§ 358-A, *et seq.* ("NHCPA"); (xxi) New Jersey's Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163, *et seq.* ("NJCSBDA"); (xxii) New York General Business Law, N.Y. Gen. Bus. Law §§349, *et seq.* ("NYGBL"); (xiii) Pennsylvania Unfair Trade Practices and Consumer Protection Law, LAW, 73 Pa. Cons. Stat. §§201-2 & 201-3, *et seq.* ("PUTPCPL").

a claim on its face “is insufficient to invoke the subject matter jurisdiction of the court,” *id.* at 358, and “does not dispute the facts alleged in the complaint,” *Davis v. Wells Fargo*, 824 F.3d 333, 346 (3d Cir. 2016). A court reviewing a facial attack must “consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff.” *Constitution Party of Pa.*, 757 F.3d at 358. Here, the Defendants invite the Court to deem their motion a factual attack and consider facts outside of the Complaint. The Court declines to do so at this time and directs the Defendants to renew their factual arguments after discovery. The Court will accept as true the pleaded facts as they relate to standing and draw all reasonable inferences in Plaintiffs’ favor. See *Constitution Party of Pa.*, 757 F.3d at 358.

2. Motion to Dismiss Under Rule 12(b)(6)

In resolving a Rule 12(b)(6) motion to dismiss, the Court accepts all pleaded facts as true, construes the complaint in the plaintiff’s favor, and determines “whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief.” *Phillips v. County of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008) (internal quotation marks and citation omitted). To survive a motion to dismiss, the claims must be facially plausible, meaning that the pleaded facts “allow [] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The allegations must be “more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

III. ANALYSIS⁷

1. Standing

Defendants argue that the Court should dismiss Plaintiffs’ claims because the FAC still fails to establish injury-in-fact for the Group III Plaintiffs. The Court disagrees.

As discussed at length in the Court’s 2021 Opinion, Plaintiffs must allege that their Personal Information was accessed, stolen, or misused to establish injury-in fact in the data breach context. See 2021 Opinion at 10-20. Each Plaintiff whom the Court previously placed in Group III has now alleged identity theft, or misuse of their information through publication on the dark web or attempted identity theft. For example, Plaintiff S. Walden now alleges that an unauthorized individual attempted to open a Charles Schwab brokerage account using her name and/or Social Security number, and Plaintiff J. Buck alleges two unauthorized charges on the credit card she provided to AMCA. FAC ¶¶ 98, 295. Further, each Plaintiff now alleges that his or her personal information has been found on the Dark Web. See, e.g., FAC ¶ 101.⁸ Accordingly, every Plaintiff has sufficiently alleged injury-in-fact such that they are either in Group I⁹ or Group II.¹⁰

⁷ The Court notes that Plaintiff Julio Antonio Perez Vieyra has voluntarily dismissed his claims against Quest and Optum. See ECF No. 569.

⁸ The Court is not convinced by Defendants’ arguments that some allegations are insufficient for failure to further specify the circumstances of phishing attempts that began after the data breach, or the information published on the dark web and when it was discovered. This level of specificity is not required at this stage, especially because the Court must accept the allegations as true and resolve inferences in favor of Plaintiffs. See *Constitution Party of Pa.*, 757 F.3d at 357. The Defendants may renew their specificity and factual causation arguments after discovery.

⁹ Group I now includes Jo Ann Buck (unauthorized charges).

¹⁰ Group II now includes: Breanna Klein, Lisa Taylor, Annie Mae Smith, Karen Copeland, Lucinda Dirks, Ashley Finch, Rose Marie Perry, LaTease Rikard, Naomi Jaworowski, Karli Parker, Deanna Taylor, Matthew DiFonzo,

Additionally, the Court’s 2021 Opinion found that the allegation that Plaintiffs “would not have had their Personal Information compromised by hackers ‘but for’ Defendants’ choice to contract with AMCA without maintaining any oversight,” was sufficient to establish causation for Article III standing at this stage. 2021 Opinion at 21. The Court finds these allegations sufficient for the Plaintiffs at issue here. See FAC ¶¶ 474-75.

The Court therefore finds that former Group III Plaintiffs, now designated as part of either Group I or Group II, and newly added Plaintiffs, have sufficiently established standing to survive the Motions to Dismiss.

2. Failure to State a Claim¹¹

In the Court’s prior Opinion, it found that all Group I and II Plaintiffs had sufficiently plead negligence and negligence per se but dismissed the breach of implied contract and unjust enrichment claims. The Court also dismissed most claims for violations of state consumer laws.¹² Here, the Court will address whether the FACs cured the deficiencies outlined in the Court’s prior opinion and the sufficiency of the FACs regarding the claims of new Group I and II Plaintiffs.

A. Negligence Claims

The Defendants argue that (1) Plaintiffs have not adequately pled the injury and damages elements of common law negligence; (2) Plaintiffs cannot premise their negligence per se claims on alleged violation of Section 5 of the FTC Act or HIPAA; and (3) Plaintiffs’ negligence per se claims are not cognizable under the law of many of Plaintiffs’ home states. The Court disagrees regarding common law negligence, and again declines to dismiss negligence per se claims prior to discovery.

Defendants do not make any arguments regarding new Group I and II Plaintiffs that the Court did not consider in its 2021 Opinion. Regarding the negligence claims, the Court found that Defendants owed Plaintiffs a duty to safeguard their Personal Information, and that Defendants breached that duty by failing to oversee AMCA’s data security. 2021 Opinion at 27-28. The Court also found that Plaintiffs’ allegations that their “Personal Information would not have been compromised but for” that breach were sufficient to establish causation, and that the injuries sufficient for standing were sufficient to allege damages at this stage. Id. at 29-30. The Court declined to address the negligence per se claims before the end of discovery and a choice of law decision. Id. at 32-33. Because the Defendants simply restate their previous negligence arguments, the Court again finds that the new Group I and II Plaintiffs have sufficiently alleged injury and damages such that their negligence and negligence per se claims may continue.¹³

Brittney Petitta (phishing attempts and/or information on dark web), and Shannon Walden (unauthorized brokerage account).

¹¹ The Court reiterates its decision that “it is premature to decide choice of law issues at this stage.” 2021 Opinion at 25. “That said, the Court may still address several arguments raised by Defendants in the Motions regarding Plaintiffs’ common law claims, where the potentially-applicable states’ laws are not meaningfully distinct.” Id. Furthermore, the parties again agree that the statutory claims should apply the law of each Plaintiff’s respective state.

¹² Specifically, the Court permitted certain claims for violations of MNCFA, CLRA, UCL, and the NJCSBDA to proceed.

¹³ The Court notes that it has reserved its determination regarding the economic loss and other differing state damages doctrines for after discovery.

B. Unjust Enrichment

Plaintiffs have not plausibly alleged an unjust enrichment claim. As discussed in detail in the 2023 Order, “[a]llegations that Plaintiffs would not have engaged Defendants for medical services do not plausibly suggest that the Personal Information itself is a part of Defendants’ business model,” such that Defendants were unjustly enriched. 2023 Order at 6. The Court will therefore dismiss the unjust enrichment claims with prejudice, as further amendment would be futile.

C. Privacy Claims

Plaintiffs have not plausibly alleged their common-law privacy claims—breach of confidence and invasion of privacy—because the FAC does not allege unauthorized disclosure as required by both claims. See Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114 (3d Cir. 2019) (Breach of confidence requires “the unconsented, unprivileged disclosure to a third party of nonpublic information.”); O’Donnell v. United States, 891 F.2d 1079, 1083 (3d Cir. 1989) (To plead invasion of privacy, Plaintiffs must plead that the Defendants “believe[d], or [was] substantially certain, that [they] lack[ed] the necessary legal or personal permission to commit the intrusive act.”).¹⁴ Although Plaintiffs argue that Quest’s disclosure of their personal information to AMCA was unauthorized, the Court is not convinced.

The FAC itself asserts that Quest’s Privacy Policy provided that it may disclose private information to an outside collection agency when necessary. FAC ¶ 331. Plaintiff’s argument that Quest provided more information than needed fails to rebut the undisputed fact that the policy permitted disclosure of private information to third parties such as AMCA when collections services were necessary. As discussed more fully in the 2023 Order, “Plaintiffs’ assertion that an ‘unauthorized disclosure occurred’ because Defendants ‘failed to implement and maintain reasonable safeguards’ sounds ‘in negligence’” rather than privacy torts. 2023 Order at 7 (citing In re Brinker Data Incident Litig., No. 3:18-CV-686-J-32, 2020 WL 691848, at *22 (M.D. Fla. Jan. 27, 2020)).¹⁵ Accordingly, the Court will dismiss the breach of confidence and invasion of privacy claims.

D. Statutory Claims¹⁶

The Defendants argue that Plaintiffs’ have failed to state violations of their respective state’s consumer and or data security statutes. Specifically, the Defendants argue that certain

¹⁴ See also 2023 Order at 6-7.

¹⁵ The Court also notes that even if these circumstances were sufficient to establish an intentional intrusion by Quest and Optum, the intrusion would not be “highly offensive to a reasonable person” as required to plead an invasion of privacy claim where Quests’ privacy policy contemplated sharing private information with bill collectors. See Christie v. Nat'l Inst. for Newman Stud., No. CV 16-6572 (FLW), 2019 WL 1916204, at *11 (D.N.J. Apr. 30, 2019) (Whether an intentional invasion is highly offensive “turns on one's reasonable expectation of privacy... a reasonable person cannot conclude that an intrusion is highly offensive' when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy.”).

¹⁶ The Court will not revisit its findings that the following Plaintiffs have pled violations of state consumer statutes: Elizabeth Hollway’s claim against Quest under the MNCFA, and Ria Jairam’s claim against Optum360 under the NJCDBA. The Court notes that the Defendants have not moved to dismiss the CLRA and UCL claims at issue here except for Plaintiff Taylor’s CLRA claim. See Quest Mem at 32 n.26.

claims fail (1) for lack of Injury and Causation¹⁷ or (2) because Plaintiffs have not alleged misrepresentations or omissions-based claims with particularity. Defendants argue that the remaining statutory claims should be dismissed based on statute-specific rules. The Court will address each statute in turn, addressing statutes together only where the analysis is identical.

a) Omission-Based Consumer Claims¹⁸

Quest first argues that Plaintiffs' omission-based statutory claims should be dismissed for failure to plead reliance or causation with the particularity required. The Court agrees in part.

As discussed at length in the Court's 2021 Opinion, Plaintiffs must plead "that they read [Quest's] privacy policies before agreeing to blood testing" to establish the reliance and/or causation elements of an omissions-based consumer fraud claim. *Id.* at 55-56, 61; *see also Tabler v. Panera LLC*, No. 19-CV-01646, 2020 WL 3544988, at *6-7 (N.D. Cal. June 30, 2020) (dismissing UCL and CLRA claims for failure to allege specific facts regarding statements). In contrast, Plaintiffs' claims based on unlawfulness or unfairness may proceed if they plausibly allege the requirements of each statute. 2021 Opinion at 39-41.

Here, Plaintiffs appear to assert omissions-based consumer protection claims under New York's NYGBL, Pennsylvania's PUTCPL, California's CLRA, Indiana's IUTPA, Iowa's ICFA, Kansas's KSA, Kentucky's KCPA, Minnesota's MNCFA, Missouri's MOMPA, and New Hampshire's NHCPA. However, most Plaintiffs do not allege that they ever read Quest's privacy Policy or received any other statement from Defendants which could have informed their decision whether to purchase lab services if not for its omission of the alleged data security risks. Plaintiff's argument that the relaxed Rule 9(b) standard permits omissions claims without such allegations is misplaced. Plaintiff must still "plausibly allege that the omission had some impact on [the] purchasing decision." 2021 Opinion at 50. Accordingly, these Plaintiffs' omissions-based consumer claims are dismissed.

Two Plaintiffs have alleged that they read Quest's privacy policies at the time that they received services. FAC ¶¶ 32, 124 (Klein-California;¹⁹ and Finch-Kansas). These Plaintiffs have sufficiently alleged reliance and causation, and therefore their omission-based statutory claims may proceed.²⁰

¹⁷ The Defendants make broad arguments that Plaintiffs statutory claims fail for lack of injury. The Court is not convinced that all of these statutes limit ascertainable loss such that the harms identified *supra* Section III.1 would be insufficient to establish damages. *See, e.g., Via Christi Reg'l Med. Ctr., Inc. v. Reed*, 298 Kan. 503, 519, 314 P.3d 852, 864 (2013) ("a consumer need not establish measurable monetary damages to qualify as aggrieved" under the KSA); *Complete Auto. Repair Servs. v. Capps*, No. 2012-CA-002145-MR, 2015 WL 2445911, at *5 (Ky. Ct. App. May 22, 2015), as modified (May 29, 2015) (concluding that "a person is not required to allege a specific amount of actual damages that he has already incurred as out-of-pocket expenses to make out a *prima facie* case under" the KCPA). Unless Defendants establish that a statute specifically limits the type of injury, the Court will not dismiss the claim for lack of injury. In the 2021 Opinion, the Court found, with respect to the statutes at issue here, the CLRA did not limit the type of injury required. The Court will address and apply each remaining statute's requirements in turn.

¹⁸ Court previously dismissed misrepresentation-based claims because (1) Optum did not make any statements or have any relationship with Plaintiffs prior to their lab services, and (2) Quest's privacy policy does not contain actionable misrepresentations. *See* 2021 opinion at 44-48. The Court's prior analysis applies here, and as a result all consumer claims are dismissed to the extent they are based on misrepresentations.

¹⁹ For consistency, the Court finds that Klein's UCL claim may proceed only to the extent it seeks restitution. 2021 Opinion at 56-58. The FAC does not include allegations suggesting a different result here.

²⁰ As none of the parties mention unconscionability, the Court finds that FAC asserts only misrepresentation or omissions-based consumer claims. As a result, the Court need not further address these claims.

b) California CMIA

The Defendants argue that CMIA claim should be dismissed because the FAC fails to allege that they mishandled Plaintiff's medical information as defined by the statute. The Court disagrees.

The Court previously held that Plaintiffs failed to allege facts sufficient to show that their "medical information" was viewed or accessed by an unauthorized person as required under the CMIA. 2021 Opinion at 63-64 (explaining that CMIA covers information "regarding a patient's medical history, mental or physical condition, or treatment"); Cal. Civ. Code § 56.05. The FAC now includes an explanation regarding Quest and Optum's transmission of patients' ICD codes, which "can be used to identify information relating to an individual's medical history, mental or physical condition, and treatment." FAC ¶ 338, 336-41. Plaintiffs allege that ICD codes related to their care were stored on the AMCA's CHAMP database that was accessed as part of the data breach. Id. ¶ 356. As discussed in more detail in the Court's 2023 Order, these clarifying allegations are sufficient for the CMIA to survive dismissal. See 2023 Order at 9-10 (addressing affirmative disclosure, authorized disclosure, and third-party oversight arguments).

In addition, Optum's factual arguments that it is not a healthcare provider, health services plan, or contractor as defined by CMIA, and that it did not engage in any relevant conduct, are unavailing. The CMIA defines a contractor as "a medical service organization [that] is not a health care service plan or provider of health care." Cal. Civ. Code § 56.05 (d). The FAC provides that Optum contracted with Quest to run Quest's revenue services operations, FAC ¶ 335, and that Optum regularly compiled and transmitted Plaintiffs' medical information to AMCA. Id. ¶ 336. These allegations suffice at this stage to establish that Optum is a contractor subject to the CMIA and therefore had a duty to safeguard Plaintiff's medical information.²¹ Accordingly, the CMIA claims of Klein and Taylor may proceed.

c) Cybersecurity and Data Breach Statutes²²

The Defendants argue that the Cyber Security and Data Breach Notification claims should be dismissed because, among other things, Plaintiffs have not alleged injury from defective notification pursuant to the Iowa IPISBPL and New Hampshire NHNSB. The Court agrees.

As a preliminary matter, the Court has already held that the KPCI may provide a private right of action, but exempts entities regulated by HIPAA, including Defendants. See 2023 Order at 12-13. As a result, the Court will also dismiss the KPCI claims here.

Plaintiffs have not alleged an injury arising from defective notification to survive the dismissal of their IPISBPL and NHNSB claims. Neither Plaintiff Dirks nor Jaworowski allege an injury other than the unauthorized access to their personal information and publication on the dark web. Unlike Plaintiff Jairam, whose \$2,000 injury from unauthorized charges could conceivably arise in part from a delay in notification by the Defendants, 2021 Opinion at 66 n. 60, Dirks and Jaworowski allege privacy injuries that arose only from the data breach itself. Defendants' delayed notification had no bearing on the publication of their information on the dark web or the subsequent phishing attempts based on that information. See, e.g., Fox v. Iowa Health Sys., 399

²¹ The lone case Optum cites to support its argument that it is not subject to the CMIA is inapposite. See Fernandez v. Leidos, Inc., 127 F. Supp. 3d 1078, 1090 (E.D. Cal. 2015) (finding, without elaboration, that an entity providing "electronic information management and data security services" was not a contractor for medical services as defined by the CMIA.). The Court is satisfied that as an entity alleged to have partnered with a healthcare provider to oversee payment and collections from patients, Optum is subject to the CMIA. Optum may renew this any other fact argument after discovery.

²² Plaintiffs withdraw their claim under the Kentucky Security Breach Notification Act. Pl. Opp. at 46.

F. Supp. 3d 780, 801 (W.D. Wis. 2019) (“Because plaintiffs do not explain how they would have suffered less damages had [Defendants] notified them sooner, the Court will dismiss their claims for violations of the breach notification statutes.”).

Accordingly, the Court will dismiss the KPCI, IPISBPL and NHNSB claims.

IV. CONCLUSION

For the reasons stated above, Defendants’ Motion to Dismiss pursuant for lack of standing to Rule 12(b)(1), ECF Nos. 349, 350, are **DENIED**.

Defendants’ Motions to Dismiss for failure to state a claim pursuant to Rule 12(b)(6), ECF Nos. 349, 350, are **GRANTED in part** and **DENIED in part**. The following claims may proceed:

- 1) The negligence and negligence per se claims of all Plaintiffs;
- 2) Elizabeth Hollway’s claim against Quest under the Minnesota Consumer Fraud Act;
- 3) Breanna Klein’s claims against Quest under the California Consumers Legal Remedies Act and the California Unfair Competition Law;
- 4) Breanna Klein and Lisa Taylor’s claims against Quest and Optum360 under the California Medical Information Act;
- 5) Ria Jairam’s claim against Optum360 under the New Jersey Customer Security Breach Disclosure Act;
- 6) Ashley Finch’s claim against Quest under the Kansas Consumer Protection Act;

Plaintiffs may amend the Complaint within 30 days of this Order to cure any deficiencies identified herein.

SO ORDERED.

/s Madeline Cox Arleo
MADELINE COX ARLEO
UNITED STATES DISTRICT JUDGE